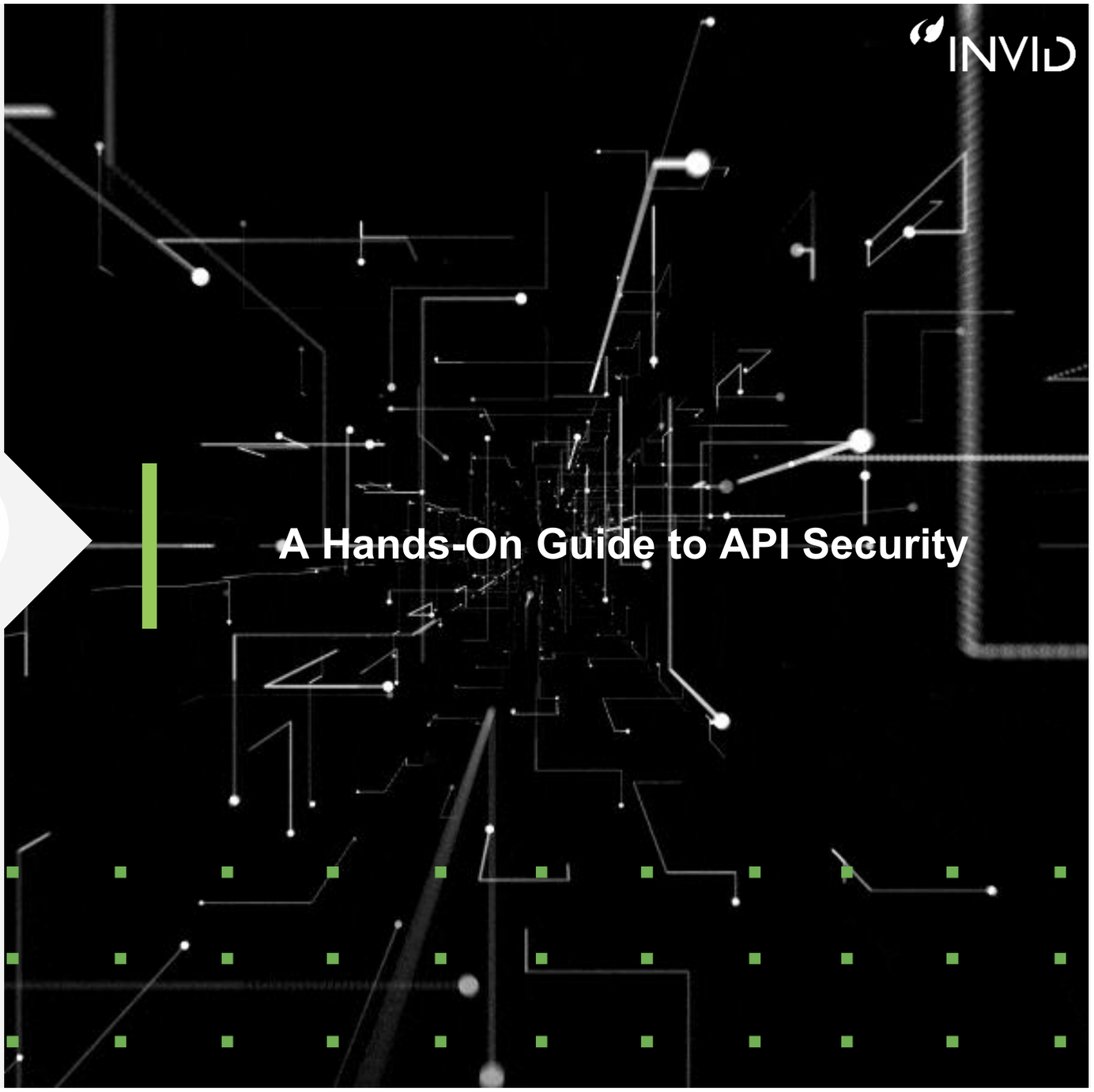
Hacking APIs: Understanding Challenges, and Best Practices



Roger Bergling

INVID

Version #1 - Copyright © INVID Jönköping AB 2025-11-01 – Alla rättigheter reserverade

Definition is a Hacker?



#whoami

Roger Bergling

INVID the last 29 years 11 month

https://www.linkedin.com/in/rogerbergling/

https://blog.invid.eu



Session Objectives

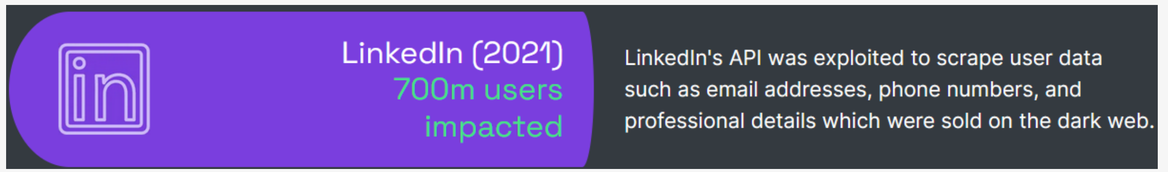
- Why we need to improve API Security
- Identify and exploit common API vulnerabilities.
- Use essential tools for API security testing.
- Conduct hands-on security testing.

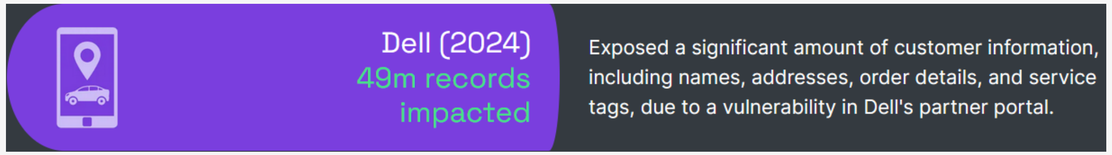


Why API Security Matters

- APIs are the backbone of modern applications, but they are a common target for attackers.

Source: https://salt.security/ and https://www.wired.com







1. Sensitive Messages Breach (January 2024): A buggy API led to unauthorized access to 650,000 sensitive messages, exposing passwords and allowing penetration testers to retrieve confidential data. This breach shows how even a single API flaw can compromise highly sensitive information.

Why API Security Matters

Dan Barahona
Co-founder, APIsec University
dan@apisecuniversity.com

API Explosion

83%

of all Internet traffic is API traffic

Akamai

APIs Under Attack

#1

"API attacks will become the **most frequent attack vector**"

Gartner

APIs Under-Secured

4%

of testing is Security



Source: stateofapis.com

Tools for API Security Testing

- Postman, Insomnia, Bruno.
- BurpSuite, mitmproxy.
- Hashcat, Kiterunner, JWT Toolkit.
- Tips for secure tool usage (e.g., avoid storing sensitive data in cloud).

OWASP/crAPI

completely ridiculous API (crAPI)







Demo Objective: Find API endpoints

Reverse Engineering an API

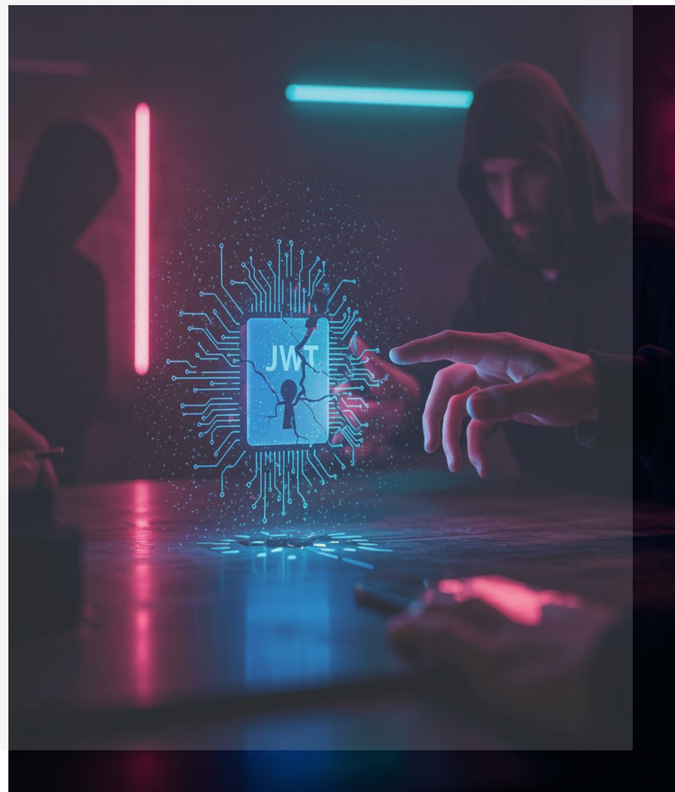
- Problem: If you do not have documentation of the API.



- Demo: Using mitmweb,mitmproxy2swagger, Bruno
- Defense/Best practices: Document you API, Rate limit your API

Demo Objective: Broken Authentication
(JWT Vulnerabilities)

- Problem: Exploiting JWT tokens through cracking and modification.
- Demo: Crack JWT tokens with Hashcat and modify tokens using JWT Toolkit.
- Defense/Best practices : Use secure token handling, rotate keys, and avoid simple passwords.



Demo Objective: BOLA

Broken Object Level Authorization

- Problem: Users have access to other user information.
- Demo: How to access other user information
- Defense/Best practices Implement robust access control on end points.



Take API Security to the Next Level!

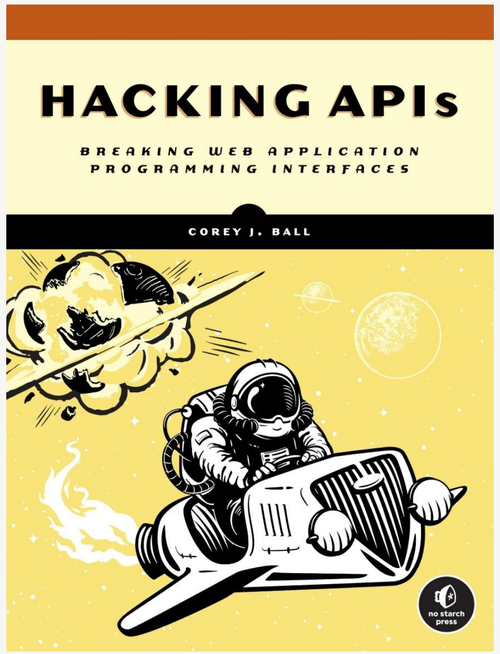
- Educate yourself almost free

https://www.apisecuniversity.com/

https://nordicapis.com/blog/

https://academy.tcm-sec.com/

https://www.home.apimasters.io/learn





Closing Notes

INVID

- Regularly pentest your APIs using tools like **https://www.apisec.ai/**
- Build security testing in your development pipelines
- Foster a security-first culture in API development and design
- Know your application or ”target” ☺

Command and Links

https://blog.invid.eu

INVID CYBERSECURITY

We secure what matters the most!



Version #1 - Copyright © INVID Jönköping AB 2025-11-01 – Alla rättigheter reserverade